PATENT ABSTRACTS OF JAPAN

(11)Publication number : 07-287514
(43)Date of publication of application : 31.10.1995

(51)Int.Cl. G09C 1/00
G06F 15/00
G06K 17/00
G06K 19/10
H04L 9/32

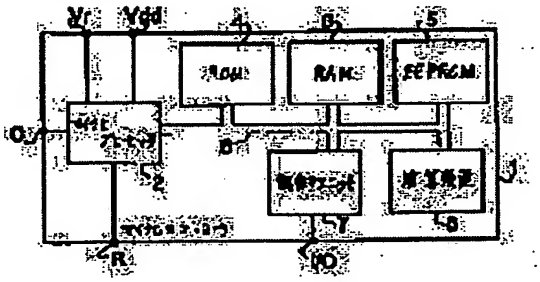
(21)Application number : 07-071464
(22)Date of filing : 29.03.1995

(71)Applicant : PHILIPS ELECTRON NV
(72)Inventor : RONALD FERREIRA
JOSEPH HOPPE

(30)Priority
Priority number : 94 9403773 Priority date : 30.03.1994 Priority country : FR

(54) MESSAGE SIGNATURE SYSTEM EXECUTING DEVICE AND CHIP CARD PROVIDED IN THE SAME

(57)Abstract:
PURPOSE: To execute an RSA-type encipher system, suitable for the existing laws for managing the civil usage of chip card.
CONSTITUTION: When the structure of a message passed through a micro- processor 2 as the parameter of an instruction matches a previously defined pattern stored in an EEPROM 5, the message is signed and outputted. When they do not match, operation is denied, and an error message is transmitted to a terminal. The respective instructions are stored in a ROM 4, and the message to be outputted is calculated by an arithmetic unit 6.



LEGAL STATUS

[Date of request for examination] 24.01.2002
[Date of sending the examiner's decision of rejection]
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]
[Date of final disposal for application]
[Patent number] 3647921
[Date of registration] 18.02.2005
[Number of appeal against examiner's decision of rejection]
[Date of requesting appeal against examiner's decision of

rejection]
[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Industrial Application] This invention relates to the message signature system activation equipment which performs the signature authentication function to the message signed [on which were signed and it message-signature-functioned] according to the RSA type protected data switching system.
[0002] Especially this invention is applied to the field of cryptocommunication which uses a chip card.
[0003] Moreover, this invention relates to a chip card equipped with the message signature system activation equipment explained in the 1st step while using a RSA type protected data switching system.
[0004]
[Description of the Prior Art] A RSA protected data switching system will be United States Patent specification 4405829th at the name of RIBESUTO, SHAMIA, and ray dolman sleeves in 1978. It is indicated by the number. This is based on the difficulty [the large number "n" which are the two prime factors "p" and the product of "q"] of factorization. According to this system, the message which should be dealt with is formed as a number of connection divided into fixed-length Brock who is under "n." Each block M is [Equation 1]. C=Me Mod(n)
since -- Code C is formed with the characteristic "e" obtained. It is shown that Mod (n) operates by the modulo "n" here. A recipient is [Equation 2] in order to decode Code C. It is [Equation 3] in order to perform Cd Mod(n) =MedMod(n) =M. It is necessary to get to know the secret characteristic "d" with which are satisfied of e-dMod{(p-1) (q-1)}=1. This system can also perform authentication of the signature of a message, and a signature. Message M is signed by the sender using a private key "d."
[Equation 4] S=Md Mod(n)
The recipient of the signed message S can attest this signature by using the public key "e" of a sender in this case.
[Equation 5] Se Mod(n) =MdeMod (n) =M [0005] A public key cryptosystem (for example, RSA type code system) is realizable by low cost with the present when the chip card progressed technically, maintaining satisfaction **** actuation. In many countries, it has tried to build the national network based on the chip card technique over the application as which the high-level secret of EDI (data information interchange), an electronic payment system, a banking system, a health system, etc. is required.
[0006] When the code system used is a powerful system in the semantics that the message enciphered by many persons other than the user of a private key cannot be decoded, there is a possibility that a part of capacity of these networks may be used for the criminal purpose. Therefore, under the current law, decode of the data of a citizen application is forbidden in principle.
[0007] Therefore, another code system by which a signature function like GQ system indicated by the France patent specification No. 2620248 for which it applied to the DSS (digital signature specification) system or November 7, 1987 when specification was defined in the United States of America was limited must be used.
[0008]
[Problem(s) to be Solved by the Invention] However, when a RSA type code system maintains very

high secret level, and is widely used for many products, and it is wanted and a permission is granted, it has the advantage that it can use as a data decode system.
[0009] Therefore, the purpose of this invention is offering the message signature system activation equipment which performs the code system of the RSA type which suited the current law which manages the citizen application of a chip card.
[0010]
[Means for Solving the Problem] For this reason, the message signature system activation equipment by this invention is characterized by equipping said message signature system activation equipment with a means to forbid the message encryption and the decryption function of a RSA type system of arbitration.
[0011] The 1st example of the message signature system activation equipment by this invention is equipped with a means to forbid the signature of the message according to said structure while it compares the structure beforehand determined according to the message of arbitration with the need of assembling with each message which should be signed.
[0012] Therefore, it prevents that can prevent signing an inaccurate more effective code message, therefore unjust decode actuation is performed. Since a code logical message is not controllable, either, even when it can be predicted, this code logical message cannot follow said structure.
[0013] Furthermore, the message signature system activation equipment by this invention outputs a display as a result of affirmation, when these two are in agreement, and when not in agreement, it is equipped with the means which can output a display as a result of negation while comparing the obtained message with said structure preferably, after attesting the signature of the signed message.
[0014] therefore, the message obtained after such signature authentication -- a result -- a display -- negation -- it is -- a case -- **** -- an outside -- outputting -- not having -- consequently, an invader cannot use the "Taira (plane)" message to signature verification actuation, in order to encipher a message unjustly.
[0015] The 2nd example of the message signature system activation equipment by this invention applies a compressibility function to all messages before a signature, outputs the message subsequently compressed and signed, and when required, it is equipped with a means to output the "Taira" message.
[0016] Therefore, the unauthorized use of the signature function as a decode function is impossible. The reason is that a compressibility function is applied to the first message.
[0017] Furthermore, the message signature system activation equipment by this invention In this case, after attesting the signature of said message compressed and signed, while comparing the compressed message which is obtained with the output "Taira" message to which said compressibility function was applied first suitably When these two are in agreement, a display is outputted as a result of affirmation, and in not being in agreement, it has the means which can output a display as a result of negation.
[0018] Therefore, the message obtained after such signature verification is not outputted when a result display is negation.
[0019]
[Example] The message signature system activation equipment by this invention is realized based on 83C852 of the microcontroller protected from a physical viewpoint, for example, Philips. It constitutes based on EEPROM5 which memorizes various data, such as ROM4 including the instruction of operation which carries out especially this invention for this kind shown in drawing 1 of microcontroller 1 with a microprocessor 2 and RAM3, a public key of a card, and a public key of the third person who exchanges data. This microcontroller 1 consists of an arithmetic unit 6 for actuation with the need of realizing a code function, and a control unit 7 for an input/output connected also to input I/O of a microcontroller 1. Said component of a microcontroller 1 is interconnected by bus 8.
[0020] A microprocessor 2 is connected also to the inputs R, C, and Vr of a microcontroller 1, and Vdd. Input R is used for receiving the reinitialization signal of a microprocessor 2. Input C receives an external clock signal. Input Vr A reference voltage signal is received. Moreover, Input Vdd receives a power-source signal.
[0021] He can understand all other details from the specification of quoted microcontroller 83C852.

[0022] As shown in drawing 2 , ROM4 is equipped with Types D1 and D2 of the right relevant to the file name and this file of EEPROM5, -, the register that has Dn, and the pointer to this file of EEPROM5 to each data files F1 and F2 of EEPROM5, -, and Fn. Therefore, in order to perform actuation of the information on the data file of EEPROM5, it is necessary to make the microprocessor 2 (drawing 1) which confirms whether the type of this data of operation was permitted pass data.
[0023] For example, EEPROM5 is equipped with the file which has the file of the public key guided at equipment, and the private key of equipment. It is shown that the right relevant to this information cannot read these rights from the exterior. Furthermore, according to this invention, the file of the guided key has the right which restricts access to the data to signature authentication actuation.
[0024] The information memorized by equipment is protected according to the structure of such an EEPROM.
[0025] In the 1st example of the message signature system activation equipment by this invention, all the "Taira" messages Mo need to follow the structure defined beforehand. In the example explained later, it selected so that it might have a specific value to the effective bit of 64 of each message Mo (magnitude of the message processed by the RSA system is made equal to 512 bits by this example.). The bit by which 64 was defined beforehand is memorized by EEPROM5. In order to promote the notation of such structure, it is advantageous to tell a regular configuration, "00-0", "11-1", and "0101-01" to EEPROM5. [for example,]
[0026] However, by repeating the predetermined part of a message, i.e., a message, two or more times, for example, it selects so that known redundancy may be put on each message Mo.
[0027] Drawing 3 shows the flow chart of actuation of the 1st example of the message signature system activation equipment by this invention. The corresponding instruction is memorized by ROM4 (drawing 1) of a microcontroller 1 (drawing 1).
[0028] The semantics of various Brock of this flow chart is explained below.
Box K1: A microprocessor 2 (drawing 1) waits for attainment of the demand to port I/O of a microprocessor 1 (drawing 1). The contents of these demands are defined as document ISO/IEC 7816-3 published in 1993, and 7816-4. ** also includes the field which has the field which shows the type of the instruction (loading of the public key to the file of a public key to which it was shown to EEPROM5 (drawing 1), a signature, authentication, or verification of a signature) which should be executed, and data which should be processed among these. Acceptance of a demand advances a procedure to a box K2.
[0029] Box K2: The test which can determine whether relate to the public key which loads an instruction. When it relates to a public key, a procedure goes to a box K3. When that is not right, it goes to a box K4.
[0030] Box K3: The public key in an instruction data field memorizes to the file of a key to which it was shown to EEPROM5 (drawing 1). Subsequently, a procedure returns to a box K1.
[0031] Box K4: The test which can determine whether relate to a signature instruction. When it relates to a signature instruction, a procedure progresses to box K5. When that is not right, it goes to a box K7.
[0032] Box K5: The test of the structure of the message Mo which passed as a parameter of an instruction. When the most effective bit of 64 of Message Mo is in agreement with the pattern which was memorized to EEPROM5 (drawing 1) and which was defined beforehand, it relates to the "Taira" message which can sign without unjust risk (a signature instruction is not barred in order to perform an unjust decryption.). A procedure is continued with a box K6 after that. When that is not right, actuation is refused, an error message is transmitted to a terminal (it is a response message by which the field "a regulation" encoded by 2 bytes defines the type of an error, as defined as the quoted document in fact.), and a procedure returns to a box K1 after that.
[0033] Box K6: Signature [several 6] Ms=(Mo)d Mod(n)
The output of the message Ms ******(ed) and signed. Subsequently, a procedure returns to a box K1.
[0034] Box K7: The test which can determine whether relate to a signature authentication instruction. When it relates to a signature authentication instruction, a procedure is continued with a box K8. When that is not right, a procedure goes to a box K11.

[0035] Box K8: Storage to RAM3 (drawing 1) with the public key "e" used for reading the file of a key to which it was shown to the signed messages Ms and EEPROM5 (drawing 1) which passed the instruction data field.
[0036] Box K9: Message [several 7] Count of Mo'=(Ms) e Mod (n).
[0037] a box -- K -- ten -- : -- a message -- Mo -- ' -- 64 -- most -- being effective -- a bit -- EEPROM -- five (drawing 1) -- memorizing -- having had -- beforehand -- giving a definition -- having had -- a pattern -- comparing -- things (box K101) -- obtaining -- having had -- a message -- Mo -- ' -- structure -- verification . When not in agreement among these two, a display is outputted with a box K103 as a result of negation (this format is the same as a format of the error message of box K5.). When these are in agreement, while memorizing message Mo' to RAM3 (drawing 1), a display is outputted to a box K102 as a result of affirmation (if it is shown that there is no error of the "regulation" field encoded by two octets and the "data" field is a request as this was also defined as the quoted document, it is a response message containing the attested message.). Subsequently, a procedure returns to a box K1.
[0038] Box K11: The test which can determine whether relate to a signature verification instruction. When it relates to a signature verification instruction, a procedure is continued with a box K12. When that is not right, a procedure goes to a box K13.
[0039] Box K12: The comparison with the "Taira" message received by the instruction data field and message Mo' memorized by RAM3 (drawing 1) (box K121). When these are the same, a display is outputted as a result of affirmation (box K122). When that is not right, a display is outputted as a result of negation (box K123). Subsequently, a procedure returns to a box K1.
[0040] Box K13: Processing of an instruction of other types which are not within the limits of this invention, therefore are not indicated here. Subsequently, a procedure returns to a box K1.
[0041] The 1st example which has the advantage of being very easy is related when the identity of coincidence is known. Therefore, the end use is [as opposed to / especially / the predetermined application determined very good] suitable.
[0042] According to the 2nd example by this invention, a compressibility function is applied to all the messages before a signature. Such a function is reference "Comment utiliser les fonctions de condensation dans la protection des donnees" published at the time of the SECURICOM seminar which there is a date on March 15, 1988 and was held in Paris in 1988. It is indicated. The main properties of such a function cannot find in fact another message which gives the irreversible and same result.
[0043] Drawing 4 shows the flow chart of actuation of the 2nd example of the message signature system activation equipment by this invention. The corresponding instruction is memorized by ROM4 (drawing 1) of a microcontroller 1 (drawing 1).
[0044] The semantics of various Brock of this flow chart is explained below.
Box K21: A microprocessor 2 (drawing 1) waits for attainment of a demand of port I/O of a microprocessor 1 (drawing 1). A procedure goes to a box K22 immediately after that.
[0045] Box K22: The test which can determine whether relate to the public key which loads an instruction. When it relates to a public key, a procedure continues with a box K23. When that is not right, it goes to a box K24.
[0046] Box K23: The public key which passed the instruction data field is memorized by the file of a key to which it was shown to EEPROM5 (drawing 1). Subsequently, a procedure returns to a box K21.
[0047] Box K24: The test which can determine whether relate to a signature instruction. When it relates to a signature instruction, a procedure continues with a box K25. When that is not right, a procedure goes to a box K28.
[0048] Box K25: Application of the compressibility function to the message Mo which passed the instruction parameter and which should sign.
[0049] Box K26: Message H (Mo) obtained by doing in this way is compressed. In this example, a RSA system processes a 512-bit fixed-length message. Therefore, it is necessary to supplement with message H (Mo) by adding the pattern Z beforehand defined in order to increase the die length of a message to 512 bits (EEPROM5 (drawing 1) memorized). Therefore, the message obtained is [Equation 8]. {M'=H(Mo)| |Z}

It becomes (notation | | shows compression actuation here.).
[0050] Box K27: Signature [several 9] Ms=(M')d Mod(n)
The output of the message Ms ******(ed) and signed. Subsequently, a procedure returns to a box K1.
[0051] Box K28: The test which can determine whether relate to a signature authentication instruction. When it relates to a signature authentication instruction, a procedure continues with a box K29. When that is not right, a procedure goes to a box K32.
[0052] Box K29: Storage to RAM3 (drawing 1) with the public key "e" which was read to the file of a key to which it was shown to the signature messages Ms and EEPROM5 (drawing 1 R> 1) which passed the instruction data field and which should be used. Box K30: Message [several 10] M"=(Ms)e Mod(n)
****** [0053] Box K31: Verification of the structure of the obtained message (box K311). This message is configuration X|. It is necessary to have |Z. Let Z be the pattern which was memorized to EEPROM5 (drawing 1) and which was defined beforehand here. When a message does not have configuration X||Z, a display is outputted as a result of negation (box K313). Otherwise, while memorizing Message X to RAM3 (drawing 1), a display is outputted as a result of affirmation (box K312). Subsequently, a procedure returns to a box K1. This authentication is the 1st check which checks that it is the message effectively signed with the private key with which the message Ms which passed as a parameter is equivalent to a public key "e."
[0054] Box K32: The test which can determine whether relate to a signature verification instruction. When it relates to a signature verification instruction, a procedure is continued with a box K33. When that is not right, a procedure goes to a box K34.
[0055] Box K33: A compressibility function H compares the "Taira" message received by the instruction data field applied first with the message memorized by RAM3 (drawing 1) (box K331). When these are the same, a display is outputted as a result of affirmation (box K332). When that is not right, a display is outputted as a result of negation (box K333). Subsequently, a procedure returns to a box K1.
[0056] Box K34: Processing of an instruction of another type which is not indicated here therefore it is not within the limits of this invention. Subsequently, a procedure returns to a box K1.
[0057] Though the 1st example obtains a completely satisfactory result, there is often the need of having the strengthening protection which can be used. Such strengthening protection is obtained especially about a signature in this 2nd example. The reason is that strengthening protection uses a compressibility function. Another advantage that the starting point of the public key which should be used in order to use a public key (it defined as the advice X509 of CCITT) assay concept and to attest the signed message can be proved also has this strengthening protection.
[0058] All the users A that own the message signature system activation equipment by this invention are actually the public key assay CA which EEPROM5 (drawing 1) memorized and was signed by the authorization AS of a system so that it might explain below. And open parameter PPA It can use.

[Equation 11]
$$C_A = [H(PP_A)]^{d_{AS}} \text{ Mod}(n_{AS})$$

In this case, [Equation 12]
$$PP_A = Id_A \parallel e_A \parallel Val_A \parallel n_A \parallel \ldots$$

It carries out (here, PPA is made into User's A open parameter, H is made into a compressibility function, IdA is made into User's A identifier, ValA is made into the date of the effectiveness User's A public key eA, and - shows other parameters in the case of the ability to take into consideration, makes nA and nAS User A and the modulo of Authorization AS, and uses dAS as the private key of Authorization AS.).
[0059] Therefore, when sending by express the message by which User A was signed to User B, User A is the open parameter PPA at the time of User's A Taira writing. And public key authentication CA It transmits. In this case, User B is User's A public key authentication CA by performing the following procedures. It can attest.

[0060] Open parameter PPA of a compressibility function H Application.
[Equation 13]
$T = C_A^{e_{AS}} \text{ Mod}(n_{AS})$

****** (let eAS be the public key of the authorization AS which can use equipment for insurance here.). The comparison with the obtained messages T and H (PPA). When in agreement, it is User's A public key eA. And modulo nA They are these public keys eA to authentication of the message which it was attested, and was signed as User B already explained. And modulo nA It can be used.
[0061] This approach of attesting the public key of the user A by User B is the public key assay CA about the above-mentioned signature authentication function in fact. While applying, it is the open parameter PPA about the above-mentioned signature assay function. It consists of applying.
[0062] Therefore, in this 2nd example of the message signature system activation equipment by this invention, it also has another advantage that authentication of a signature and authentication of a user's public key before verification are verifiable.
[0063] In the another example, a decode function can be attested only to a predetermined user. For this reason, it is enough just to relate each private key to the use standard of the decode limited to the predetermined user.
[0064] Before testing the structure of the obtained message to the 1st example, the structure of the message which tested the value of this use standard to the box K10, therefore was obtained is verified only when decode actuation is forbidden.
[0065] To the 2nd example, a decode instruction is arranged in a box K34, and said instruction is executed after the test of the property of the use standard of the private key contained in the private key file of EEPROM5.
[0066] Drawing 5 shows a data switched system equipped with two chip cards A and B, and forms the message signature system activation equipments A1 and B1 by this invention in each of these chip cards. Each holder of these two chip cards communicates through a terminal C1.
[0067] A health system is mentioned as an actual example of application of such a system. A patient's individual card is made into a chip card A, the individual card of a special medical examination of health to a patient's file is formed by the chip card B, and information interchange is performed through the terminal C1 with which a doctor's premise has been arranged.
[0068] In Table 1, it is between [of these three] components, namely, the example of the exchange protocol to the 2nd example of the message signature system activation equipment by this invention is shown (I1, I2, I3, and I4 are considered as a display as a result of the affirmation sent by express to the terminal C1 with each card B after actuation, or negation.).
[Table 1]

カードA	端末C 1	カードB
署名Mo		
←		
送信M_{SA}		
→		
要求C_A，PP_A		
←		
	認証C_A	
	→	
	表示I 1	
	I 1が 検証PP_A	
	肯定 →	
	表示I 2	
	←	
	I 2が 認証M_{SA}	
	肯定 →	
	表示I 3	
	←	
	I 3が 認証M_{SA}	
	肯定 →	
	表示I 4	
	←	
	終了	

[0069] It is clear that the above-mentioned example can be changed within the limits of this invention.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] It is message signature system activation equipment characterized by to have a means to by_which said message signature system activation equipment forbids the message encryption and the decryption function of a RSA type system of arbitration in the message signature system activation equipment which performs the signature authentication function to the message signed [on which were signed and it message-signature-functioned] according to the RSA type protected data switching system.
[Claim 2] Said message signature system activation equipment is message signature system activation equipment according to claim 1 characterized by having the structure beforehand determined according to the message of arbitration with the need of assembling, and a means to forbid the signature of the message according to said structure while comparing each message (Mo) which should be signed.
[Claim 3] Said message signature system activation equipment is message signature system activation equipment according to claim 2 which outputs a display as a result of affirmation when these two are in agreement, and is characterized by to have the means which can output a display as a result of negation when not in agreement while comparing the obtained message (Mo') with said structure, after attesting the signature of the signed message (Ms).
[Claim 4] Said message signature system activation equipment is message signature system activation equipment according to claim 1 characterized by having a means to apply a compressibility function (H) to all messages (Mo) before a signature, and to output the message (Ms) subsequently compressed and signed, and to output the "Taira" message (Mo) in being required.
[Claim 5] The compressed message which is obtained after said message signature system activation equipment attests the signature of said message (Ms) compressed and signed (X), While said compressibility function (H) compares the output "Taira" message (Mo) applied first Message signature system activation equipment according to claim 4 characterized by having the means which outputs a display as a result of affirmation when these two are in agreement, and can output a display as a result of negation when not in agreement.
[Claim 6] Message signature system activation equipment according to claim 5 characterized by performing a public key assay (CA) concept and a open parameter (PPA), and attesting the received public key (eA and nA) using the means of the preceding clause.
[Claim 7] Message signature system activation equipment given in any 1 term of the claims 1-6 characterized by enabling it to permit a decode function to a number of users which the use standard was related to each private key, and were limited.
[Claim 8] It is the chip card characterized by said chip card equipping any 1 term of the claims 1-7 with the message signature system activation equipment of a publication in the chip card using a RSA type protected data switching system.

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平7－287514

(43)公開日　平成７年(1995)10月31日

(51)Int.Cl.*	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０９Ｃ　1/00		9364－5L		
Ｇ０６Ｆ　15/00	３３０　Ｅ	7459－5L		
Ｇ０６Ｋ　17/00	Ｖ			
			Ｇ０６Ｋ　19/00	Ｓ
			Ｈ０４Ｌ　9/00	Ａ

審査請求　未請求　請求項の数８　ＯＬ　（全８頁）　最終頁に続く

(21)出願番号　特願平7－71464

(22)出願日　平成７年(1995)３月29日

(31)優先権主張番号　９４０３７７３

(32)優先日　1994年３月30日

(33)優先権主張国　フランス（ＦＲ）

(71)出願人　590000248
フィリップス　エレクトロニクス　ネムローゼ　フェンノートシャップ
ＰＨＩＬＩＰＳ　ＥＬＥＣＴＲＯＮＩＣＳ　Ｎ．Ｖ．
オランダ国　アインドーフェン　フルーネヴァウツウエッハ　1

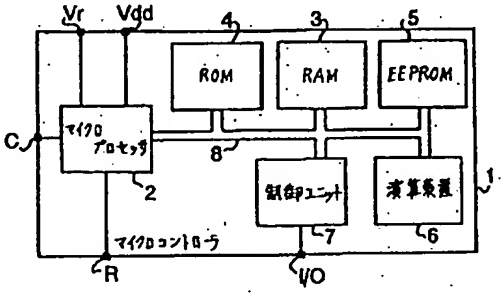
(72)発明者　ロナルド　フェレイラ
フランス国　75013　パリ　リュ　デュノワ　56

(72)発明者　ヨゼフ　ホッペ
フランス国　91470　レ　モリエール　リュ　デ　ボア　1　ビス

(74)代理人　弁理士　杉村　暁秀　（外５名）

(54)【発明の名称】　メッセージ署名システム実行装置及びこれを具えるチップカード

(57)【要約】
【目的】　チップカードの市民用途を管理する現行法に適合したＲＳＡタイプの暗号システムを実行する。
【構成】　命令のパラメータとしてマイクロプロセッサ２を通過したメッセージの構造が、ＥＥＰＲＯＭ５に記憶した予め定義されたパターンに一致する場合、メッセージの署名及び出力を行う。これらが一致しない場合、動作が拒絶され、エラーメッセージが端末に送信される。各命令はＲＯＭ４に記憶されており、出力されるメッセージの計算は演算装置６で行われる。



1

【特許請求の範囲】

【請求項1】　ＲＳＡタイプの保護データ交換システムに従ってメッセージ署名機能及び署名されたメッセージに対する署名認証機能を実行するメッセージ署名システム実行装置において、前記メッセージ署名システム実行装置は、任意のＲＳＡタイプのシステムのメッセージ暗号化及び復号化機能を禁止する手段を具えることを特徴とするメッセージ署名システム実行装置。

【請求項2】　前記メッセージ署名システム実行装置は、組み立てる必要のある任意のメッセージに従って予め決定された構造と、署名されるべき各メッセージ（Ｍｏ）とを比較するとともに、前記構造に従わないメッセージの署名を禁止する手段を具えることを特徴とする請求項1記載のメッセージ署名システム実行装置。

【請求項3】　前記メッセージ署名システム実行装置は、署名されたメッセージ（Ｍｓ）の署名を認証した後、得られたメッセージ（Ｍｏ'）と前記構造とを比較するとともに、これら二つが一致する場合には肯定の結果表示を出力し、かつ、一致しない場合には否定の結果表示を出力することができる手段を具えることを特徴とする請求項2記載のメッセージ署名システム実行装置。

【請求項4】　前記メッセージ署名システム実行装置は、署名前に圧縮関数（Ｈ）を全てのメッセージ（Ｍｏ）に適用し、次いで圧縮かつ署名されたメッセージ（Ｍｓ）を出力し、必要な場合には「平」メッセージ（Ｍｏ）を出力する手段を具えることを特徴とする請求項1記載のメッセージ署名システム実行装置。

【請求項5】　前記メッセージ署名システム実行装置は、前記圧縮かつ署名されたメッセージ（Ｍｓ）の署名を認証した後、得られる圧縮されたメッセージ（Ｘ）と、前記圧縮関数（Ｈ）が最初に適用された出力「平」メッセージ（Ｍｏ）とを比較するとともに、これら二つが一致する場合には肯定の結果表示を出力し、かつ、一致しない場合には否定の結果表示を出力することができる手段を具えることを特徴とする請求項4記載のメッセージ署名システム実行装置。

【請求項6】　前項の手段を用いて、公開鍵検定（C_A）概念及び公開パラメータ（PP_A）を実行し、受信された公開鍵（e_A，n_A）を認証するようにしたことを特徴とする請求項5記載のメッセージ署名システム実行装置。

【請求項7】　使用規準を各秘密鍵に関連させて、限定された数の使用者に対して復号機能を許可することができるようにしたことを特徴とする請求項1から6のうちのいずれか1項に記載のメッセージ署名システム実行装置。

【請求項8】　ＲＳＡタイプの保護データ交換システムを利用するチップカードにおいて、前記チップカードは、請求項1から7のうちのいずれか1項に記載のメッセージ署名システム実行装置を具えることを特徴とするチップカード。

2

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は、ＲＳＡタイプの保護データ交換システムに従ってメッセージ署名機能及び署名されたメッセージに対する署名認証機能を実行するメッセージ署名システム実行装置に関するものである。

【０００２】本発明は特にチップカードを用いる暗号通信の分野に適用されるものである。

【０００３】また本発明は、ＲＳＡタイプの保護データ交換システムを利用するとともに第1段で説明したメッセージ署名システム実行装置を具えるチップカードに関するものである。

【０００４】

【従来の技術】ＲＳＡ保護データ交換システムは、リベスト、シャミア及びエイドルマンの名で１９７８年に米国特許明細書第4405829 号に開示されている。これは、二つの素数“ｐ”及び“ｑ”の積である大きな数“ｎ”の因数分解の困難さに基づいている。このシステムによれば、取り扱うべきメッセージは、“ｎ”未満である固定長のブロックに分割された数の連接として形成されている。各ブロックＭは、

【数1】$C = M^e \bmod (n)$

から得られる指数“ｅ”により暗号Ｃを形成する。ここでＭｏｄ（ｎ）は動作をモジュロ“ｎ”で行うことを示す。暗号Ｃを復号するために、受信人は、

【数2】$C^d \bmod (n) = M^{ed} \bmod (n) = M$

を行うために、

【数3】$e \cdot d \bmod \{(p-1)(q-1)\} = 1$

を満足する秘密指数“ｄ”を知る必要がある。このシステムは、メッセージの署名及び署名の認証も行うことができる。メッセージＭは、秘密鍵“ｄ”を用いて送信人により署名される。

【数4】$S = M^d \bmod (n)$

署名されたメッセージＳの受信人はこの場合、送信人の公開鍵“ｅ”を用いることによりこの署名を認証することができる。

【数5】$S^e \bmod (n) = M^{de} \bmod (n) = M$

【０００５】チップカードが技術的に進歩した現在では、満足いく動作を維持しながら公開鍵暗号システム（例えばＲＳＡタイプの暗号システム）を低コストで実現することができる。多くの国では、ＥＤＩ（データ情報交換）、電子支払システム、銀行システム、健康システム等のようなハイレベルの秘密が要求される用途に対するチップカード技術に基づく国家ネットワークを構築するのを試みている。

【０００６】用いられる暗号システムが、秘密鍵の使用者以外の何人も暗号化されたメッセージを復号することができないという意味で強力なシステムである場合、これらのネットワークの容量の一部が犯罪の目的に用いら

れるおそれがある。したがって、現行法では原則的に市民用途のデータの復号を禁止している。

【０００７】したがって、アメリカ合衆国で規格が定められたＤＳＳ（デジタル署名規格）システム又は１９８７年１１月７日に出願されたフランス特許明細書第2620248号に記載されたＧＱシステムのような署名機能が限定された別の暗号システムを用いなければならない。

【０００８】

【発明が解決しようとする課題】しかしながら、ＲＳＡタイプの暗号システムは、非常に高い秘密レベルを保ち、多数の製品に広く用いられ、所望されかつ許可される場合にはデータ復号システムとして用いることができるという利点を有する。

【０００９】したがって本発明の目的は、チップカードの市民用途を管理する現行法に適合したＲＳＡタイプの暗号システムを実行するメッセージ署名システム実行装置を提供することである。

【００１０】

【課題を解決するための手段】このために、本発明によるメッセージ署名システム実行装置は、前記メッセージ署名システム実行装置は、任意のＲＳＡタイプのシステムのメッセージ暗号化及び復号化機能を禁止する手段を具えることを特徴とするものである。

【００１１】本発明によるメッセージ署名システム実行装置の第１例は、組み立てる必要のある任意のメッセージに従って予め決定された構造と、署名されるべき各メッセージとを比較するとともに、前記構造に従わないメッセージの署名を禁止する手段を具える。

【００１２】したがって、不正により、有効な暗号メッセージの署名が行われるのを防ぐことができ、したがって不正な復号動作が実行されるのを防止する。暗号論理メッセージは予言可能でも制御可能でもないので、この暗号論理メッセージは前記構造に従うことができない。

【００１３】さらに、本発明によるメッセージ署名システム実行装置は好ましくは、署名されたメッセージの署名を認証した後、得られたメッセージと前記構造とを比較するとともに、これら二つが一致する場合には肯定の結果表示を出力し、かつ、一致しない場合には否定の結果表示を出力することができる手段を具える。

【００１４】したがって、このような署名認証後に得られたメッセージは、結果表示が否定である場合には外側に出力されず、その結果、侵入者は、メッセージを不正に暗号化するために、署名検証動作に対し「平（プレーン）」メッセージが使用できない。

【００１５】本発明によるメッセージ署名システム実行装置の第２例は、署名前に圧縮関数を全てのメッセージに適用し、次いで圧縮かつ署名されたメッセージを出力し、必要な場合には「平」メッセージを出力する手段を具える。

【００１６】したがって復号機能としての署名機能の不正使用は不可能である。その理由は、圧縮関数が最初のメッセージに適用されるからである。

【００１７】さらに、本発明によるメッセージ署名システム実行装置は、この場合好適には、前記圧縮かつ署名されたメッセージの署名を認証した後、得られる圧縮されたメッセージと、前記圧縮関数が最初に適用された出力「平」メッセージとを比較するとともに、これら二つが一致する場合には肯定の結果表示を出力し、かつ、一致しない場合には否定の結果表示を出力することができる手段を具える。

【００１８】したがって、このような署名検証の後得られたメッセージは、結果表示が否定である場合には出力されない。

【００１９】

【実施例】本発明によるメッセージ署名システム実行装置を、物理的な観点から保護されたマイクロコントローラ、例えばフィリップス社の83C852に基づいて実現する。図１に示すこの種のマイクロコントローラ１を、マイクロプロセッサ２と、ＲＡＭ３と、特に本発明を実施する動作命令を含むＲＯＭ４と、カードの公開鍵、データを交換する第三者の公開鍵等のような種々のデータを記憶するＥＥＰＲＯＭ５とに基づいて構成する。このマイクロコントローラ１は、暗号機能を実現する必要のある動作用の演算装置６と、マイクロコントローラ１の入力Ｉ／Ｏにも接続された入力／出力用の制御ユニット７とからも構成される。マイクロコントローラ１の前記素子をバス８により相互接続する。

【００２０】マイクロプロセッサ２を、マイクロコントローラ１の入力Ｒ，Ｃ，V_r，V_{dd}にも接続する。入力Ｒを、マイクロプロセッサ２の再初期化信号を受信するのに用いる。入力Ｃは外部クロック信号を受信する。入力V_rは基準電圧信号を受信する。また、入力V_{dd}は電源信号を受信する。

【００２１】他の全ての詳細を、引用したマイクロコントローラ83C852の仕様書から理解することができる。

【００２２】図２に示すように、ＥＥＰＲＯＭ５の各データファイルＦ１，Ｆ２，　，Ｆｎに対して、ＲＯＭ４は、ＥＥＰＲＯＭ５のファイル名及びこのファイルに関連する権利のタイプＤ１，Ｄ２，　，Ｄｎを有するレジスタと、ＥＥＰＲＯＭ５のこのファイルに対するポインタとを具える。したがって、ＥＥＰＲＯＭ５のデータファイルの情報の動作を実行するために、このデータの動作のタイプが許可されたか否かチェックするマイクロプロセッサ２（図１）にデータを通過させる必要がある。

【００２３】例えば、ＥＥＰＲＯＭ５は、装置に案内される公開鍵のファイル及び装置の秘密鍵を有するファイルを具える。この情報に関連する権利は、これらの権利を外部から読み出せないことを示す。さらに本発明によれば、案内された鍵のファイルは、署名認証動作に対するデータへのアクセスを制限する権利を有する。

【００２４】このようなＥＥＰＲＯＭの構造により、装置に記憶された情報を保護する。

【００２５】本発明によるメッセージ署名システム実行装置の第１実施例では、全ての「平」メッセージＭｏは、予め定義された構造に従う必要がある。後に説明する例では、各メッセージＭｏの６４の有効なビットに対して特定の値を持つように選定した（ＲＳＡシステムで処理されるメッセージの大きさを、本例では５１２ビットに等しくする。）。６４の予め定義されたビットはＥＥＰＲＯＭ５に記憶される。このような構造の記法を促進するために、規則的な形状、例えば“００　０”，“１１　１”，“０１０１　０１”をＥＥＰＲＯＭ５に伝えるのが有利である。

【００２６】しかしながら、例えばメッセージすなわちメッセージの所定の部分を複数回繰り返すことにより、各メッセージＭｏに既知の冗長を置くように選定する。

【００２７】図３は、本発明によるメッセージ署名システム実行装置の第１実施例の動作のフローチャートを示す。対応する命令は、マイクロコントローラ１（図１）のＲＯＭ４（図１）に記憶されている。

【００２８】このフローチャートの種々のブロックの意味を以下説明する。

ボックスＫ１：マイクロプロセッサ２（図１）はマイクロプロセッサ１（図１）のポートＩ／Ｏへの要求の到達を待つ。これらの要求の内容は、１９９３年に発行されたドキュメントISO/IEC 7816-3及び7816-4に定義されている。これらの内容は、実行すべき（ＥＥＰＲＯＭ５（図１）の案内された公開鍵のファイル、署名、認証又は署名の検証への公開鍵のロード）命令のタイプを示すフィールド及び処理すべきデータを有するフィールドも含む。要求が受理されると、手続はボックスＫ２に進む。

【００２９】ボックスＫ２：命令をロードする公開鍵に関連するか否かの決定を行うことができるテスト。公開鍵に関連する場合、手続はボックスＫ３に進む。そうでない場合、ボックスＫ４に進む。

【００３０】ボックスＫ３：命令データフィールド中の公開鍵が、ＥＥＰＲＯＭ５（図１）の案内された鍵のファイルに記憶する。次いで、手続がボックスＫ１に戻る。

【００３１】ボックスＫ４：署名命令に関連するか否かの決定を行うことができるテスト。署名命令に関連する場合、手続はボックスＫ５に進む。そうでない場合には、ボックスＫ７に進む。

【００３２】ボックスＫ５：命令のパラメータとして通過したメッセージＭｏの構造のテスト。メッセージＭｏの６４の最も有効なビットが、ＥＥＰＲＯＭ５（図１）に記憶した予め定義されたパターンに一致する場合、不正の危険なく署名することができる「平」メッセージに関連する（署名命令は、不正な復号化を行うために妨げられない。）。その後手続がボックスＫ６で継続される。そうでない場合、動作が拒絶され、エラーメッセージが端末に送信され（それは実際には、引用された文書に定義されたように、２バイトに符号化されたフィールド「規則」がエラーのタイプを定義する応答メッセージである。）、その後手続がボックスＫ１に戻る。

【００３３】ボックスＫ６：署名

【数６】Ｍｓ＝（Ｍｏ）^{d} Ｍｏｄ（ｎ）

の計算及び署名されたメッセージＭｓの出力。次いで、手続がボックスＫ１に戻る。

【００３４】ボックスＫ７：署名認証命令に関連するか否かの決定をすることができるテスト。署名認証命令に関連する場合、手続がボックスＫ８で継続される。そうでない場合、手続がボックスＫ１１に進む。

【００３５】ボックスＫ８：命令データフィールドを通過した署名されたメッセージＭｓと、ＥＥＰＲＯＭ５（図１）の案内された鍵のファイルを読み出すのに用いる公開鍵“ｅ”とのＲＡＭ３（図１）への記憶。

【００３６】ボックスＫ９：メッセージ

【数７】Ｍｏ’＝（Ｍｓ）^{e} Ｍｏｄ（ｎ）の計算。

【００３７】ボックスＫ１０：メッセージＭｏ’の６４の最も有効なビットとＥＥＰＲＯＭ５（図１）に記憶された予め定義されたパターンとを比較する（ボックスＫ１０１）ことにより得られたメッセージＭｏ’の構造の検証。これら二つの間で一致しない場合、否定の結果表示をボックスＫ１０３にて出力する（このフォーマットはボックスＫ５のエラーメッセージのフォーマットと同一である。）。これらが一致する場合、メッセージＭｏ’をＲＡＭ３（図１）に記憶するとともに肯定の結果表示をボックスＫ１０２に出力する（これも、引用された文書に定義されたように、２オクテットに符号化された「規則」フィールドがエラーのないことを示し、「データ」フィールドが所望なら認証されたメッセージを含む応答メッセージである。）。次いで、手続はボックスＫ１に戻る。

【００３８】ボックスＫ１１：署名検証命令に関連するか否かの決定を行うことができるテスト。署名検証命令に関連する場合、手続をボックスＫ１２で継続する。そうでない場合、手続はボックスＫ１３に進む。

【００３９】ボックスＫ１２：命令データフィールドに受信された「平」メッセージと、ＲＡＭ３（図１）に記憶されたメッセージＭｏ’との比較（ボックスＫ１２１）。これらが同一である場合、肯定の結果表示が出力される（ボックスＫ１２２）。そうでない場合、否定の結果表示が出力される（ボックスＫ１２３）。次いで、手続がボックスＫ１に戻る。

【００４０】ボックスＫ１３：本発明の範囲内ではなく、したがってここでは記載しない他のタイプの命令の処理。次いで、手続がボックスＫ１に戻る。

【００４１】非常に簡単であるという利点を有する第１

実施例は、一致の恒等式が既知である場合に関連するものである。したがって、最終使用が非常に良好に決定された所定の用途に対して特に好適である。

【００４２】本発明による第２実施例によれば、圧縮関数が、署名前のあらゆるメッセージに適用される。このような関数は、１９８８年３月１５日の日付があり、１９８８年にパリで開催されたＳＥＣＵＲＩＣＯＭセミナーの時に出版された文献"Comment utiliser les fonctions de condensation dans la protection des donnees" に記載されている。このような関数の主要な特性は、実際には不可逆であり、同一の結果を与える別のメッセージを見つけることができない。

【００４３】図４は、本発明によるメッセージ署名システム実行装置の第２実施例の動作のフローチャートを示す。対応する命令は、マイクロコントローラ１（図１）のＲＯＭ４（図１）に記憶されている。

【００４４】このフローチャートの種々のブロックの意味を以下説明する。

ボックスＫ２１：マイクロプロセッサ２（図１）はマイクロプロセッサ１（図１）のポートＩ／Ｏの要求の到達を待つ。その後手続がすぐにボックスＫ２２に進む。

【００４５】ボックスＫ２２：命令をロードする公開鍵に関連するか否かの決定を行うことができるテスト。公開鍵に関連する場合、手続がボックスＫ２３で継続する。そうでない場合、ボックスＫ２４に進む。

【００４６】ボックスＫ２３：命令データフィールドを通過した公開鍵が、ＥＥＰＲＯＭ５（図１）の案内された鍵のファイルに記憶される。次いで、手続がボックスＫ２１に戻る。

【００４７】ボックスＫ２４：署名命令に関連するか否かの決定を行うことができるテスト。署名命令に関連する場合、手続がボックスＫ２５で継続する。そうでない場合、手続がボックスＫ２８に進む。

【００４８】ボックスＫ２５：命令パラメータを通過した署名すべきメッセージＭｏへの圧縮関数の適用。

【００４９】ボックスＫ２６：このようにして得られたメッセージＨ（Ｍｏ）が圧縮される。本例では、ＲＳＡシステムは５１２ビットの固定長のメッセージを処理する。したがって、メッセージの長さを５１２ビットに増やすために、例えば（ＥＥＰＲＯＭ５（図１）に記憶された）予め定義されたパターンＺを加えることにより、メッセージＨ（Ｍｏ）を補足する必要がある。したがって、得られるメッセージは、

【数８】 {M' ＝Ｈ（Ｍｏ）｜ ｜Ｚ}

となる（ここで記号｜ ｜は圧縮動作を示す。）。

【００５０】ボックスＫ２７：署名

【数９】 $Ms = (M')^{d} \bmod (n)$

の計算及び署名されたメッセージＭｓの出力。次いで、手順がボックスＫ１に戻る。

【００５１】ボックスＫ２８：署名認証命令に関連するか否かの決定を行うことができるテスト。署名認証命令に関連する場合、手続がボックスＫ２９で継続する。そうでない場合、手続がボックスＫ３２に進む。

【００５２】ボックスＫ２９：命令データフィールドを通過した署名メッセージＭｓと、ＥＥＰＲＯＭ５（図１）の案内された鍵のファイルに読み出された用いられるべき公開鍵“ｅ”とのＲＡＭ３（図１）への記憶。ボックスＫ３０：メッセージ

【数１０】 $M'' = (Ms)^{e} \bmod (n)$

の計算

【００５３】ボックスＫ３１：得られたメッセージの構造の検証（ボックスＫ３１１）。このメッセージは、形状Ｘ｜ ｜Ｚを有する必要がある。ここでＺを、ＥＥＰＲＯＭ５（図１）に記憶した予め定義されたパターンとする。メッセージが形状Ｘ｜ ｜Ｚを有しない場合、否定の結果表示が出力される（ボックスＫ３１３）。さもなければ、メッセージＸをＲＡＭ３（図１）に記憶するとともに肯定の結果表示を出力する（ボックスＫ３１２）。次いで、手続がボックスＫ１に戻る。この認証は、パラメータとして通過したメッセージＭｓが公開鍵“ｅ”に相当する秘密鍵によって有効に署名されたメッセージであることを確認する第１チェックである。

【００５４】ボックスＫ３２：署名検証命令に関連するか否かの決定を行うことができるテスト。署名検証命令に関連する場合、手続はボックスＫ３３で継続する。そうでない場合、手続はボックスＫ３４に進む。

【００５５】ボックスＫ３３：圧縮関数Ｈが最初に適用された命令データフィールドに受信される「平」メッセージと、ＲＡＭ３（図１）に記憶されたメッセージとを比較する（ボックスＫ３３１）。これらが同一である場合、肯定の結果表示を出力する（ボックスＫ３３２）。そうでない場合、否定の結果表示を出力する（ボックスＫ３３３）。次いで、手続がボックスＫ１に戻る。

【００５６】ボックスＫ３４：本発明の範囲内でない、したがってここでは記載しない別のタイプの命令の処理。次いで、手続がボックスＫ１に戻る。

【００５７】第１実施例が完全に満足な結果を得るとしても、利用できる強化保護を有する必要がしばしばある。このような強化保護はこの第２実施例で特に署名に関して得られる。その理由は、強化保護は圧縮関数を利用するからである。この強化保護は、（ＣＣＩＴＴ の勧告Ｘ５０９で定義された）公開鍵検定概念を使用し、署名されたメッセージを認証するために用いられるべき公開鍵の始点を証明することができるという別の利点も有する。

【００５８】実際に、本発明によるメッセージ署名システム実行装置を所有するあらゆる使用者Ａは、以下説明するように、ＥＥＰＲＯＭ５（図１）に記憶され、システムの許可ＡＳによって署名された公開鍵検定C_A及び公開パラメータPP_Aを利用することができる。

【数１１】

9

$$C_A = [H(PP_A)]^{d_{AS}} \mathrm{Mod}(n_{AS})$$

この場合、

【数１２】

$$PP_A = Id_A \parallel e_A \parallel Val_A \parallel n_A \parallel \cdots$$

とする（ここで、ＰＰA を使用者Ａの公開パラメータとし、Ｈを圧縮関数とし、ＩｄA を使用者Ａの識別子とし、ＶａｌA を使用者Ａの公開鍵eA の有効性の日付とし、　は考慮することができる場合の他のパラメータを示し、nA 及びnAS を使用者Ａ及び許可ＡＳのモジュロとし、dAS を許可ＡＳの秘密鍵とする。）。

【００５９】したがって、使用者Ａが、署名されたメッセージを使用者Ｂに急送する場合、使用者Ａは使用者Ａの平香込み時の公開パラメータＰＰA 及び公開鍵認証CA も送信する。この場合使用者Ｂは、以下の手順を実行することにより使用者Ａの公開鍵認証CA を認証することができる。

【００６０】圧縮関数Ｈの公開パラメータＰＰA への適用。

【数１３】

$$T = C_A^{e_{AS}} \mathrm{Mod}(n_{AS})$$

の計算（ここでeAS を、装置を安全に利用できる許可ＡＳの公開鍵とする。）。得られたメッセージＴとＨ（ＰＰA ）との比較。一致する場合、使用者Ａの公開鍵eA 及びモジュロnA が認証され、使用者Ｂは、既に説明したように、署名されたメッセージの認証に対してこれら公開鍵eA 及びモジュロnA を使用することができる。

【００６１】使用者Ｂによる使用者Ａの公開鍵を認証するこの方法は、実際には上記署名認証機能を公開鍵検定CA に適用するとともに、上記署名検定機能を公開パラメータＰＰA に適用することからなる。

【００６２】したがって本発明によるメッセージ署名システム実行装置のこの第２実施例では、署名の認証及び検証の前に使用者の公開鍵の認証の検証を行うことができるという別の利点も有する。

【００６３】別の実施例では、復号機能を所定の使用者に対してのみ認証することができる。このために、所定の使用者に限定された復号の使用規準に各秘密鍵を関連させるだけで十分である。

【００６４】第１実施例に対しては、得られたメッセージの構造をテストする前に、ボックスＫ１０に対してこの使用規準の値のテストを行い、したがって得られたメッセージの構造は、復号動作が禁止された場合のみ検証される。

【００６５】第２実施例に対しては、ボックスＫ３４に復号命令を配置し、ＥＥＰＲＯＭ５の秘密鍵ファイルに含まれる秘密鍵の使用規準の性質のテストの後に前記命令の実行を行う。

【００６６】図５は、二つのチップカードＡ及びＢを具

10

えるデータ交換システムを示し、これらのチップカードのそれぞれに、本発明によるメッセージ署名システム実行装置Ａ１及びＢ１を設ける。これら二つのチップカードの各ホルダは端末Ｃ１を介して通信を行う。

【００６７】このようなシステムの実際の適用例として健康システムを挙げる。患者の個人カードをチップカードＡとし、患者のファイルに対する健康の専門的な診療の個人カードをチップカードＢで形成し、医者の既述事項が配置された端末Ｃ１を介して情報交換が行われる。

【００６８】表１において、これら三つの素子間の、すなわち本発明によるメッセージ署名システム実行装置の第２実施例に対する交換プロトコルの例を示す（Ｉ１，Ｉ２，Ｉ３及びＩ４を、各動作後カードＢにより端末Ｃ１に急送された肯定又は否定の結果表示とする。）。

【表１】

カードA	端末C１	カードB
		署名Mo
	←	
送信M_{oA}		
	→	
要求C_A，PP_A		
	←	
		認証C_A
		→
		表示Ｉ１
Ｉ１が		検証PP_A
肯定		→
		表示Ｉ２
		←
Ｉ２が		認証M_{oA}
肯定		→
		表示Ｉ３
		←
Ｉ３が		認証M_{oA}
肯定		→
		表示Ｉ４
		←
終了		

【００６９】本発明の範囲内で上記実施例の変更を行うことができるのは明らかである。

【図面の簡単な説明】

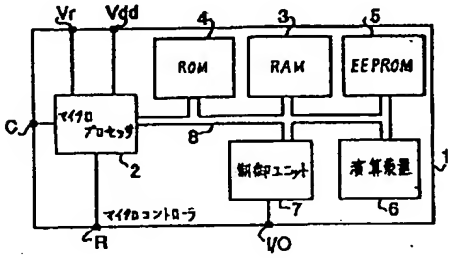
【図１】本発明によるメッセージ署名システム実行装置の線図的に示す図である。

【図２】本発明によるメッセージ署名システム実行装置の記憶装置の構造を線図的に示す図である。

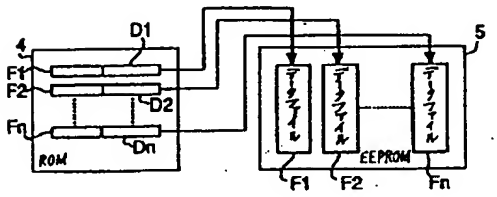
11　　12

【図３】本発明によるメッセージ署名システム実行装置の第１実施例の動作のフローチャートである。
【図４】本発明によるメッセージ署名システム実行装置の第２実施例の動作のフローチャートである。
【図５】本発明によるメッセージ署名システム実行装置を具えるチップカードを線図的に示す図である。
【符号の説明】
1　マイクロコントローラ
2　マイクロプロセッサ
3　ＲＡＭ
4　ＲＯＭ
5　ＥＥＰＲＯＭ
6　演算装置
7　制御ユニット
8　バス
A，Ｂ　チップカード
Ａ１，Ｂ１　メッセージ署名システム実行装置
Ｃ，Ｉ／Ｏ，Ｒ，V_{dd}，V_r　入力
Ｄ１，Ｄ２，Ｄｎ　権利
Ｆ１，Ｆ２，Ｆｎ　データファイル
Ｋ１，Ｋ２，Ｋ３，Ｋ４，Ｋ５，Ｋ６，Ｋ７，Ｋ８，Ｋ９，Ｋ１０，Ｋ１１，Ｋ１２，Ｋ１３，Ｋ２１，Ｋ２２，Ｋ２３，Ｋ２４，Ｋ２５，Ｋ２６，Ｋ２７，Ｋ２８，Ｋ２９，Ｋ３０，Ｋ３１，Ｋ３２，Ｋ３３，Ｋ３４，Ｋ１０１，Ｋ１０２，Ｋ１０３，Ｋ１２１，Ｋ１２２，Ｋ１２３，Ｋ３１１，Ｋ３１２，Ｋ３１３，Ｋ３３１，Ｋ３３２，Ｋ３３３　手続

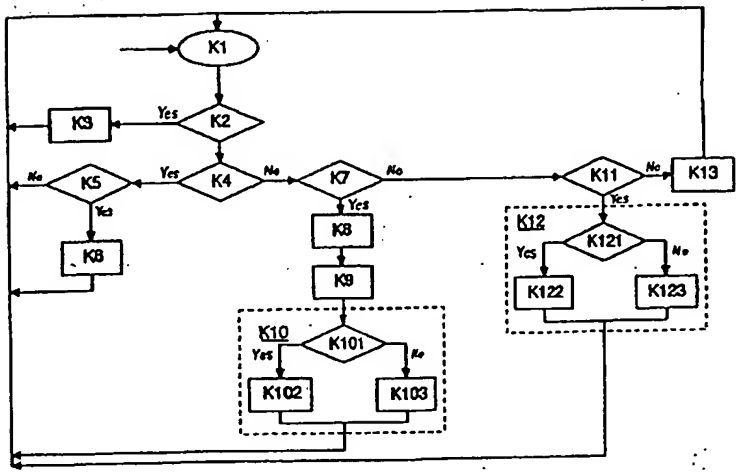
【図１】



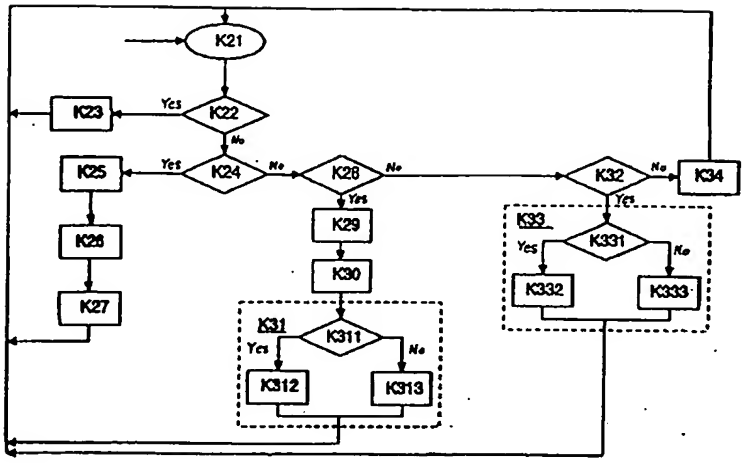
【図２】



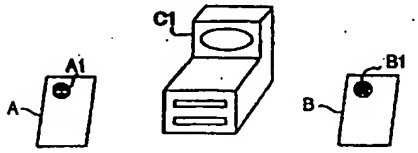
【図３】



【図4】



【図5】



フロントページの続き

(51)Int.Cl.[6]	識別記号	庁内整理番号	F I	技術表示箇所
G06K 19/10				
H04L 9/32				